TESTIMONY OF C. STEWART VERDERY, JR
ASSISTANT SECRETARY FOR BORDER AND TRANSPORTATION SECURITY POLICY AND PLANNING
DEPARTMENT OF HOMELAND SECURITY
BEFORE THE HOUSE AVIATION SUBCOMMITTEE

May 19, 2004

Chairman Mica and other distinguished Members, it is a pleasure to appear before you today to discuss how the Department of Homeland Security (DHS) is using biometrics to improve aviation security and facilitate legitimate trade and travel, particularly in the US-VISIT and Transportation Worker Identity Credential (TWIC) programs.

No single problem area has mobilized government and private sector activity in the area of identification systems as much as global terrorism. More than two years after September 11, exploration and actual implementation of the use of biometrics to ensure identity and enhance security continues to be an area of fevered activity in both the domestic and international arenas.

Biometrics is the science of identifying, recording and matching unique physical characteristics to individuals. There are five basic technologies: facial recognition, fingerprint, hand geometry, iris recognition and voice recognition.

The creation of DHS has allowed agencies to rethink security procedures and, in many cases, adapt IT infrastructures to include new biometric technologies.

US-VISIT is a Border and Transportation Security (BTS) program that represents a continuum of security measures that uses biometrics as a key element. Both State and DHS use biometrics and biographic data to check individual visa applicants against appropriate “lookout” data. In addition, these biometric technologies such as digital, inkless fingerscans and digital photographs also enable DHS to determine whether the person applying for entry to the United States is the same person who was issued a visa by the State Department.

Areas where DHS is currently exploring the potential for biometrics to enhance aviation security include Transportation Security Administration’s (TSA) recently announced award of grants to explore using biometric technologies to enhance airport security access controls, TSA’s Registered Traveler Pilot Program, and the Transportation Worker Identification Credential program. For all of these programs, TSA is working with TSA’s privacy officer and the DHS privacy officer to ensure that all relevant privacy considerations are taken into account.

TSA's will test Anti-Piggybacking technology (technology that would prevent someone from gaining access through a control point by following immediately after with someone else’s identification) and other technologies, advanced video surveillance technology and various biometric technologies to ensure that only authorized personnel have access to non-passenger controlled areas. Under the TWIC program, TSA is assessing how smart card technology that incorporates a biometric feature could be used to enhance the security of transportation facilities nationwide, including seaports, rail and transit facilities, airports and others. TSA's Registered Traveler Pilot program is enabling TSA to explore technological solutions associated with positive identity verification, including biometrics, to facilitate the movement of passengers who have received a prior security assessment through airport security checkpoints.

I will discuss all of these initiatives in greater detail below.

US-VISIT

In 1996 and 2000, the United States Congress mandated the creation of an electronic entry-exit system to manage the entry and departure of foreign visitors. After the events of September 11, 2001, Congress added the requirement that the entry exit system have the capability to confirm identity. DHS has established the US-VISIT Program to accomplish these statutory mandates and to achieve the following goals:

- Enhance the safety of our citizens and visitors;
- Facilitate legitimate travel and trade;
- Ensure the integrity of our immigration system; and
- Protect the privacy of travelers to the United States.

US-VISIT represents a major milestone in enhancing our nation's security and our efforts to reform our borders. It is a significant step towards bringing integrity back to our immigration and border enforcement systems. It is also leading the way for incorporating biometrics into international travel security systems.

US-VISIT is a continuum of security measures that begins before individuals enter the United States and continues through their arrival and departure from the country. Enrolling travelers in US-VISIT using biometric identifiers allows DHS to:

- Conduct appropriate security checks: We conduct checks of visitors against appropriate lookout databases available to consular officers and inspectors, including biometric-based checks.
- Freeze identity of traveler: We biometrically enroll visitors in US-VISIT – freezing the identity of the traveler and tying that identity to the travel document presented.
- Match traveler identity and document: We biometrically match that identity and document, with the information collected by State, enabling the inspector to determine whether the traveler complied with the terms of her/his previous admission and is using the same identity.
- Document arrivial, and departure: We collect automated arrival and departure information on travelers.
- Determine overstays: We will use collected information to determine whether individuals have overstayed the terms of their admission. This information will be

used to determine whether an individual should be apprehended or whether the individual should be allowed to enter the U.S. upon her/his next visit.

The Department of Homeland Security with the Department of State Consular Affairs have created an entire continuum of identity verification measures that begins overseas collecting fingerprints, when a traveler applies for a visa, and continues upon entry and exit from this country. The system stores biometric and biographic data in a secure, centralized database and uses travel and identity documents to access that information for identity verification and watchlist checks. Today, more than 130 visa-issuing posts have begun to capture fingerscans and digital photographs of foreign nationals when they apply for visas, regardless of their country of origin. We expect that this process will be in place at all 211 visa-issuing posts worldwide by October 2004.

At the U.S. border, certain visitors are required to provide biometric data, biographic data, and/or other documentation. This data is checked against US-VISIT databases, which contain visa issuance information, watchlists, including information from the Federal Bureau of Investigation, and immigration status information allowing border inspectors to verify identity and identify security threats and immigration violators. In its first 4 months of operation, DHS processed nearly 3.65 million foreign national applicants for admission through US-VISIT at its air and sea ports of entry. During that period, 291 individuals were identified by biometrics alone as being the subject of a lookout. DHS took adverse action in 43% of the 291 cases. Of the 291 hits, 62% were for criminal violations (some of which were immigration related criminal violations, such as previous deportation); 38% were for immigration violations alone.

One of the US-VISIT Program's primary roles is to identify those individuals who have overstayed the terms of their admission. Currently, our exit procedures are based upon receiving departure information from passenger manifests shared with us by air carriers under Custom and Border Protection's (CBP) Advanced Passenger Information System (APIS). We match information received under APIS with admission information when a passenger applies for entry into the U.S. at the port of entry, and identify those likely to have overstayed the terms of their admission. We are testing our ability to enhance matching of arrival and departure records by using biometrics in various pilot programs, one of them being at the Baltimore-Washington International Airport. We plan to expand our pilot program to a total of 15 air and seaports over the next several months. We will pilot test three options and evaluate the results to identify the best, most efficient and effective process.

At various points in the pre-entry, entry, status management and exit processes, decision makers are supported by systems checks against data from law enforcement and intelligence sources that identify persons of interest for various violations. All names and fingerscans are checked against watch lists to identify known or suspected terrorists, criminals and immigration violators.

In just a few months, the first release of US-VISIT has improved the security of our citizens and visitors. Our CBP Officers are saying that the new tools we have put in place truly help them do their jobs more effectively and are a major advancement in border control. US-VISIT adds, on average, only fifteen seconds to the average inspection time. Included in this processing time are the collection of the biometric and biographic information, the comparison of that information with that collected by the Department of State at the time of visa issuance, and the screening of the biographic and biometric information through watchlists and other criminal history information.

US-VISIT is working. We intercepted a fugitive who had escaped from prison over 20 years ago. We caught and extradited a felon wanted for manslaughter in San Diego. We finally stopped one drug dealer who had entered the U.S. more than 60 times in the past four years using different names and dates of birth. We continue to identify criminals every day at our borders, and since January 19, we have supplied crucial biometric information to our partners at the Department of State to help prevent ineligible visa applicants from obtaining a visa.

The increase in security has not had negative effect on our wait times or our commitment to service. But you don’t have to take my word for it. Albert Park, a Korean visiting his sister and arriving at John F. Kennedy International Airport, told the New York Sun (January 6th edition): "I expected a lot more delays, but it was all pretty smooth." He went on to state that "[US-VISIT] definitely makes me feel safer."

"We at the airport believe that this is a true enhancement," said Bruce Drum, associate director of the Miami-Dade County Aviation Department.” (The Associated Press, January 5th)

The Washington Post (January 6th) also reported on travelers’ perceptions of the additional security measures: “Some travelers who were fingerprinted and photographed at airports across the country yesterday said the security procedures were swift, and most said they were resigned to the new rules. ‘I don't really mind,’ said D.C. resident Salome Nnanga, a native of Ethiopia. ‘I think it's a very, very good idea to protect the country.’”

We want to ensure that we continue to be a welcoming nation, a nation that invites visitors to study, do business, and relax in our country. We also owe it to our citizens and visitors to deny entry to persons wishing to do harm, or who are inadmissible to the U.S. Few would dispute that these steps are necessary.

As we evaluate the first four months of the program, it seems clear that visitors appreciate the effort we are making to deliver security while simultaneously facilitating the process for law-abiding, legitimate travelers. We must continue to respect our visitors’ privacy, treat them fairly, and enable them to pass through inspection quickly so they can enjoy their visit in our country. As people attempt to enter our country, we must know who they are and whether we have information that they have committed a crime that would make them inadmissible to the U.S. The ability of US-VISIT to rapidly screen applicants, using biometrics, means we can have security and control without impeding legitimate travelers, and we can also help protect our welcomed visitors by drastically reducing the possibility of identity theft. Moreover, as visitors leave the country, we must know that they have not overstayed their period of authorized stay.

But we are not finished. This is a complicated job that will take time to complete. In fact, US-VISIT is designed to be rolled out in increments to ensure that the foundation is strong and the building blocks are effective. With the deployment of the entry components at air and sea ports, we have made a strong beginning, and we plan to meet the December 31, 2004, deadline to deploy US-VISIT at the 50 busiest land border ports of entry. We also expect to deploy biometric capabilities at those ports of entry to allow DHS to check the identity of certain travelers against watchlists and databases. We are seeing that we can accomplish what we set out to do: keep out criminals and terrorists, enhance the integrity of our immigration system, facilitate legitimate travel and trade and help protect the privacy and identity of our visitors.

An obvious concern for all legitimate travelers is that criminals may use their lost or stolen travel documents to enter the United States. Biometric identifiers make it difficult for criminals to travel on someone else's travel documents. This is a significant benefit that US-VISIT delivers for the millions of legitimate travelers we welcome each year. In addition, we must continue to respect our visitors' privacy. We have a Privacy Impact Assessment (PIA) being reviewed by external audiences and DHS has the first statutorily created Chief Privacy Officer, Nuala O'Connor Kelly. Ms. O'Connor Kelly along with the US-VISIT privacy officer has worked closely with privacy experts at the Office of Management and Budget, and with independent privacy consultants to prepare a PIA that addresses the beginning increments of this program.

The Department is not doing this alone. We are collaborating with other government agencies, most notably the Department of State, to implement US-VISIT and inform the traveling public. We are working closely with the air and sea travel industry regarding the requirements of the US-VISIT program, as well as speaking with constituencies along the land borders. We see our relationship with these groups as a partnership.

We are also partnering with private industry to develop the best technological solutions. In accordance with our published schedule, a Request for Proposals (RFP) was issued in November 2003. The RFP incorporates an acquisition strategy to ensure that the latest available technologies will be incorporated into US-VISIT. We expect to award the contract for this technology later this month.

An important part of the program is public education. Travelers are educated about the program before they arrive at the port of entry. We are engaged in a worldwide campaign to inform them. This campaign includes public service announcements, signage at ports of entry, explanatory cards on airplanes and cruise ships, news media coverage and on-board explanatory videos.

US-VISIT is critical to our national security as well as our economic security, and its introduction has been successful. We are committed to building a system that enhances the integrity of our immigration system by catching the few and expediting the many, and we recognize that the United States is leading the way in helping other countries around the world keep their borders secure and their doors open.

AIRPORT ACCESS CONTROL PILOT PROGRAM (AACPP)

The second BTS program that is exploring biometrics technology is the Airport Access Control Pilot Program within TSA. The Aviation and Transportation Security Act (ATSA) required the establishment of pilot programs at no fewer than 20 airports to test and evaluate new and emerging technology for providing access control and other security protections for closed or secure areas of the airports. ATSA also states that the technologies to be evaluated under the pilot programs may include, among others, biometric technologies. To meet this requirement, TSA has developed a two-phase pilot program, for which awards for Phase I were recently announced.

Phase I of the pilot includes testing of various off-the-shelf technologies, including biometric technologies including fingerprint, under a variety of real-world operational environments. Based on that analysis, TSA will then determine which technologies will be evaluated in the Phase II airports. The Phase I pilot programs will focus on identifying the operational payoffs achievable through increased use of biometric and other technologies.

In selecting airports for participation, TSA began contacting airports in October 2002 to gauge their level of interest in the program. TSA asked the 82 airports that expressed preliminary interest to complete a survey so TSA could determine how well each applicant airport fit the desired characteristics and evaluate the airport authority and management's willingness to cooperate in the pilot. Of the 55 that responded to the surveys by October 28, 2003, TSA conducted further analysis and site surveys to choose airports for participation in phase I of the program.

In selecting technologies for assessment under the pilot program, TSA issued a request for information in December, 2002. More than 350 individuals submitted technology candidates for consideration.

For Phase I, which is funded at $8,000,000, TSA announced on May 3, 2004, the selection of eight airports:

- *Boise Air Terminal/Gowen Field Airport* will test a system that combines fingerprint biometric and Radio Frequency Identification (RFID) technology to control vehicle access.
- *Miami International Airport* will test a new defense system that will incorporate intelligent video analysis and other technology to detect intruders at the perimeter.
- *Minneapolis-St. Paul International Airport* will demonstrate a detection system using intelligent video analysis to differentiate between persons who are authorized and not authorized access to secured areas of the airport.
- *Newark International Airport* will test a system using fingerprint biometric technology to allow only authorized persons in secure areas of the airport.

- *Savannah International Airport* will focus on intelligent video surveillance technology to allow only authorized personnel to operate a cargo elevator that provides access to secure areas of the airport.
- *Southwest Florida International Airport* will evaluate new RFID and wireless fingerprint biometric technology intended to enhance the level of security at a vehicle gate.
- *T. F. Green State Airport* (in Providence, RI) will focus on controlling access to a secure area via an iris biometric recognition system. In addition, the entrance will employ anti-piggy backing detection (stopping more than one vehicle from gaining entrance at a time).
- *Tampa International Airport* will test the viability of portable card readers and fingerprint recognition technology at a vehicle gate.

Two additional airports will be selected at a later date, for a total of 10 Phase I airports. Various technology will be tested during Phase I including combining fingerprint biometric and Radio Frequency Identification (FRID) technology to control vehicle access; incorporating intelligent video analysis and other technology to detect intruders and unauthorized access; and controlling access to a secure area via an iris biometric recognition system. Phase I projects will be completed by December, 2004.

After Phase I and Phase II (which will expand on the number of technologies tested in additional airport operating environments) are both completed, information gathered during these pilot projects will be made available to appropriate airport and aviation industry representatives so that they may make informed decisions when designing access control systems to meet their security and regulatory needs. TSA will also make the results of these pilot projects available to other program areas within DHS, as well as other government agencies that may have a need for designing systems that provide facility security and/or establish programs using the various technologies evaluated, including biometric technologies. TSA and US-VISIT have collaborated closely to leverage expertise within the programs.

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

TSA, through its TWIC program, is testing alternatives for developing and/or implementing a secure credential that could be used to mitigate potential threats posed by workers in transportation industries with fraudulent identification. The TWIC program is intended to enhance security controls applicable to the variety of transportation personnel whose duties require unescorted access to secure areas.

TSA has proceeded with development of the TWIC program in four phases. The first and second phases—planning and technology evaluation—have been completed. The technology evaluation phase consisted of testing at transportation facilities in the Philadelphia/Delaware River Basin and Los Angeles / Long Beach pilot program sites. During this phase, cards utilizing various technologies were issued to transportation workers with access to the facilities, and card technology performance data was collected. This phase led to TSA's selection of the Integrated Circuit Chip (ICC) technology as most suitable in the tested operational environments. The ICC is based on the National Institute of Standards and Technology (NIST) Government Smart Card Specification, includes encryption, secret keys, and active defenses, and can house a securely embedded biometric.

Phase III—the prototype phase—will involve evaluation of a broad range of business processes pertaining to identity management. These processes include enrollment of the applicants including the collection of biometrics, verification of claimed identity, and relevant checks of background information. Operational testing and evaluation will be conducted to select the biometric(s) to be used for the reference biometrics on the credential. A Request for Proposals (RFP) to begin the Prototype Phase of the Transportation Worker Identification Credential program was issued on May 10, 2004. The Prototype Phase is scheduled to last approximately seven months, and will be followed by Phase IV – implementation.

The TWIC program is being designed to leverage existing local facility control systems to the maximum extent possible, and has the potential to improve both commerce and security by providing "one credential mobility" across a number of different facilities. Decisions on how to implement a credentialing system will follow an assessment by DHS of the various prototype efforts. Our assessment will look at the cost and benefit of different approaches; most importantly how these benefit security.

REGISTERED TRAVELER PROGRAM

Finally, I will turn to the Registered Traveler (RT) Pilot Program, on which I know this Subcommittee has expressed keen interest even before enactment of ATSA and creation of the TSA.

As I mentioned before, TSA's pilot testing for a Registered Traveler program is designed to determine the feasibility of providing expedited movement through airport security checkpoints for travelers who volunteer to provide enough information about themselves to receive a security assessment indicating that they do not pose a threat to aviation security. Volunteers who participate in the RT Pilot program will also be requested to submit personal data, possibly including biometrics that will be used to validate identity using relevant government databases. Participants in the program will still be required to submit to screening for weapons, explosives, and prohibited items at the checkpoint.

TSA has collaborated with key internal and external stakeholders regarding the feasibility of such a program. Based upon interest expressed, TSA intends to conduct RT Pilots at a limited number of airports beginning in June, 2004. The pilots will last approximately 90 days. On April 5, 2004, TSA issued the first of a two-part Request for Proposal (RFP) soliciting input from the private sector for implementing Registered Traveler Pilots, and on May 13, 2004, TSA issued the second of a two-part RFP to those vendors that submitted the most highly rated capability statement to the initial Registered Traveler RFP. Awards for the Pilot operations will be made in mid-June 2004.

TSA awaits the results of the Pilot program prior to determining the feasibility and effectiveness of a broader implementation, including what costs, if any, would be incurred by those passengers who wish to participate in a future phase of the voluntary program. Upon conclusion of the pilots, results will be analyzed to ascertain security and customer service benefits and to determine the best approach for proceeding.

Conclusion

The Department is working, with its partners, to bring our nation's immigration and transportation security system into the 21st century. Technology must be utilized to move toward achieving the President's goal of secure U.S. borders and open doors to legitimate trade and travel.

Biometrics identifiers in the form of photographs and fingerprints have long played a key role in securing transportation systems and facilities; however human matching is subject to high costs and slow performance. The advent of automated matching capability gives us the ability to improve performance and permit the deployment and use of new technologies in new ways to assist us in freezing or fixing identities of foreign nationals, improve document security, and deter illegal access. In order to maximize our return on investment, it is vital that federal agencies and associated industries, also responsible for security of infrastructure, work together to create compatible systems.